December 13, 2013

Mr. Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: Comments of the American Public Power Association and the Large Public Power Council on the Preliminary Cybersecurity Framework

Dear Mr. Sedgewick:

The American Public Power Association ("APPA") and the Large Public Power Council ("LPPC") (together, "APPA-LPPC") submit these comments jointly in response to the notice and request for comments on the Preliminary Cybersecurity Framework, released by the National Institute of Standards and Technology ("NIST") on October 22, 2013 in response to Executive Order 13636.[1]

APPA and LPPC represent publicly owned electric utilities within the electric subsector that will be asked to adopt the voluntary industry methodologies, procedures and processes in the final Cybersecurity Framework. These member utilities, along with representatives of APPA and LPPC, have been active participants in the workshops that NIST has sponsored leading to publication of the Preliminary Framework.[2]

In addition to the general, policy-oriented comments on the Preliminary Framework set forth below, APPA-LPPC have developed detailed, substantive edits to the proposed framework. See Attachments A, B and C to these comments. APPA-LPPC also join in and support the Energy Sector comments filed jointly today by American Gas Association (AGA), American Public Power Association (APPA), Edison Electric Institute (EEI), Electric Power Supply Association (EPSA), GridWise Alliance (GWA), Large Public Power Council (LPPC), National Rural Electric Cooperative Association (NRECA), Utilities Telecom Council (UTC), .

[1] ''Executive Order 13636—Improving Critical Infrastructure Cybersecurity," 78 FR 11739 (February 19, 2013).

[2] APPA and LPPC also filed comments in response to NIST's February 26, 2013 Request for Information, as signatories to the Electric Power Sector Coalition Comments and the Comments of the Electric Trade Associations, both dated April 8, 2013.

APPA-LPPC members have a long history of excellence in providing reliable and affordable service, and a proven commitment to maintaining high standards as technology evolves. Cybersecurity is central to the day-to-day operations of our member utilities across the country, each of which manages cybersecurity programs tailored to its unique operations, assets and communications networks. Each of our members is committed to working with their respective suppliers of equipment, fuel and other inputs to the electricity supply chain and with their electricity end-use customers to enhance the protection and resiliency of the nation's critical infrastructure from cyber attack.

APPA-LPPC welcome NIST's development of a broad, cross-sector Baseline Framework to reduce cybersecurity risk to critical infrastructure.[3] An appropriately structured framework will provide the potential for meaningful improvement in national security, as common procedures and processes are implemented across sectors. Our members are fully committed to assisting in the development and implementation of the Framework and to participating in the processes leading to further refinements.

I. Identity of APPA and LPPC

APPA is the national service organization representing the interests of not-for-profit, publicly owned electric utilities throughout the United States. More than 2,000 public power utilities provide over 15 percent of all kilowatt-hour sales of electricity to ultimate customers, and do business in every state except Hawaii.

LPPC represents 26 of the largest state and municipal-owned utilities in the nation. Together, LPPC's members represent 90 percent of the transmission investment owned by non-federal public power entities.

Notices and communications regarding these comments may be addressed to:

AMERICAN PUBLIC POWER ASSOCIATION
Allen Mosher
Vice President of Policy Analysis
and Reliability Standards
(202) 467-2944
amosher@publicpower.org

Delia Patterson
Assistant General Counsel
DPatterson@publicpower.org

Nathan Mitchell
Director, Electric Reliability Standards and
Compliance

LARGE PUBLIC POWER COUNCIL
Jonathan D. Schneider
Jonathan P. Trotta
STINSON MORRISON HECKER LLP
1775 Pennsylvania Ave. NW, Suite 800
Washington, DC 20006-4605
(202) 728-3034
jschneider@stinson.com
jtrotta@stinson.com

Counsel for Large Public Power Council

[3] EO at section 7.

(202) 467-2925
nmitchell@publicpower.org

1875 Connecticut Ave. NW, Suite 1200
Washington, DC 20009

II. Comments

A. Efficacy of the Preliminary Framework in Achieving Objectives and Proposed Revisions to Sections 2 and 3.

The Note to Reviewers preceding the content of the Preliminary Framework asks a series of questions eliciting general comments on the efficacy of the document in defining outcomes, enabling cost effective implementation, providing useful tools to senior executives and guidance to businesses of varied types. Specifically, NIST asks:

Does the Preliminary Framework:

- *adequately define outcomes that strengthen cybersecurity and support business objectives?*
- *enable cost-effective implementation?*
- *appropriately integrate cybersecurity risk into business risk?*
- *provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?*
- *provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?*

As a general matter, APPA-LPPC believe the Preliminary Framework does a commendable job of outlining the core functions, practices and organizational attributes associated with effective programs for identifying, managing and responding to Cybersecurity Risks. APPA-LPPC recognize the substantial challenge inherent in an effort to draw program components in sufficient detail to provide substantive guidance, while remaining sufficiently flexible to apply across sectors of the economy with very diverse cybersecurity risk profiles and needed responses. The general approach taken by the Preliminary Framework in outlining the core elements of an effective program, and recommending that their application be tailored to reflect each organization's unique business requirements, risks, risk tolerance and resources makes sense to us, as it simultaneously provides useful guidance and essential flexibility.

With that said, APPA-LPPC recommend certain significant language changes to Sections 2 and 3 of the Preliminary Framework (Framework Tiers and How to Use the Framework). These changes are designed to clarify the meaning and intent of the Tiers, and to outline the provisions governing use of the Framework in terms that APPA-LPPC believe are more concrete and manageable than the current draft. The proposed revisions to the Tiers clarify that the choice of an appropriate Tier is the province of the affected entity. Further, the revisions more closely tie increasing levels of accomplishment to the functions and categories identified in the

Framework Core. The proposed revisions to Section 3 of the Preliminary Framework (How to Use the Framework) are designed to clarify that the Framework is designed to provide organizations with a systematic method for identifying their cyber risks, their risk tolerance and security aspirations, and then to proceed to construct a program to achieve specified security objectives.

These changes are reflected on the redline of the Preliminary Framework submitted herewith as Attachments A and B, and are also reflected on the Excel template (Attachment C)

B. Informational References

NIST asks whether the Preliminary Framework "express[es] existing practices in a manner that allows for effective use." On this point, APPA-LPPC believe the Preliminary Framework would be meaningfully improved by incorporating NERC's Critical Infrastructure Protective ("CIP") standards into the Informative References expressed in Appendix A (Framework Core). As electric utilities which own or operate facilities that are part of the Bulk Electric System and subject to Section 215 of the Federal Power Act ("FPA"), 16 U.S.C. 824o, many of APPA's and LPPC's members are subject to electric reliability standards developed by the North American Electric Reliability Corporation ("NERC"). These NERC standards were developed through an exhaustive industry consensus-based standards development process accredited by the American National Standards Institute ("ANSI").

NERC's Critical Infrastructure Protection ("CIP") standards impose mandatory and enforceable requirements on owners and operators of the Bulk Electric System. Compliance with the CIP standards is enforceable by NERC, subject to the oversight and approval of the Federal Energy Regulatory Commission ("FERC"). Enforcement actions may entail the imposition of financial penalties of up to one million dollars per violation per day, as well as NERC remedial action directives to ensure immediate changes to cybersecurity practices and procedures.

The NERC CIP standards are prescriptive and comprehensive, covering both cybersecurity and the physical security of cyber systems that are used to control the Bulk Electric System. Currently effective Version 3 of the NERC CIP standards are grouped as follows:

- CIP-002-3 – Critical Cyber Asset Identification
- CIP-003-3 – Security Management Controls
- CIP-004-3 – Personnel & Training
- CIP-005-3 – Electronic Security Perimeters
- CIP-006-3 – Physical Security of Critical Cyber Assets
- CIP-007-3 – Systems Security Management
- CIP-008-3 – Incident Reporting and Response Planning
- CIP-009-3 – Recovery Plans for Critical Cyber Assets

Version 5 of the NERC CIP standards was approved by FERC on November 22, 2013, to become mandatory and enforceable on April 1, 2016. As NERC explained in response to NIST's Request for Information, Version 5 of the CIP Standards reflects existing NIST guidelines (SP800-53)[4] by scaling the level of needed security controls to identified risks and providing for ongoing monitoring, assessments and corrections of controls. Version 5 of the NERC CIP standards also adds two standards to the NERC CIP family, fashioned from pre-existing requirements:

- CIP-010-1 – Configuration Change Management and Vulnerability Assessments
- CIP-011-1 – Information Protection

APPA-LPPC note that the EO expressly states that the NIST Framework "shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[5] Further, the RFI states that "[t]he Framework would be designed to be compatible with existing regulatory authorities and regulations."[6]

APPA-LPPC understand that NIST has decided, at least provisionally, not to list the CIP standards as informative cross references, on the ground that they are specific to the electricity sub-sector. APPA-LPPC ask NIST to reconsider this approach for two reasons. First, APPA-LPPC believe the CIP standards will be a useful reference point for sectors other than electricity. APPA-LPPC cannot see that other sectors are in any way prejudiced by incorporation of these provisions into the informative references. The references would in no way undermine other sector-specific frameworks, nor would the we object to further cross references to other sector standards.

Second, there is good reason to consider the electric sector to be unique, not only due to the fact that it is governed by comprehensive, mandatory standards, but also because the industry has been uniquely singled out as a target for cyber attacks. The Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reports that in the first half of 2013 some 53% of all reported cyber attacks were on the energy sector, followed in prevalence by 32% on Critical Manufacturing, and 5% each for the next most targeted sectors (communications and transportation). These figures support considering the electric sector somewhat uniquely.

[4] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, updated May 1, 2010, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[5] EO, Section 7.

[6] NIST RFI at 13025.

C. Necessary Limitations on Use of the Framework

APPA-LPPC ask NIST to state in the Introduction to the Framework or elsewhere that the Framework is not designed to be used by third parties to grade performance or provide a basis for any form of certification. Though the structure of the Framework would seem to make this evident, APPA-LPPC have been involved in discussions in which parties have pressed for some mechanism for entity performance evaluation under the Framework.

The concept behind the Tiers in the Framework and the construct of the Profiles is to encourage self-assessment by entities, based on internal evaluation of the risks they face, their risk tolerance, and their aspirations. This approach does not lend itself to external evaluation, the assessment of a pass-fail grade or any type of certificate of approval. Indeed, the use of the Framework as a tool for third-party evaluation would be counter-productive, as it would lead to the ossification of industry practices and encouraging entities to manage to compliance, instead of looking to the Framework as a guidepost for continuous improvement. As well, the prospect of any type of formal evaluation would make the potential for conflicting directions with respect to other standards acute. This is a particular concern for the electric sector as it bears on NERC CIP compliance. While APPA-LPPC members see the Framework, as it is evolving, to be generally compatible with the CIP standards, there are certainly areas where differences language and approach raise the potential for conflicting direction. If the Framework is employed in support of evaluations which have regulatory or legal consequences, it raises the potential for conflicting direction and confusion. APPA-LPPC urge NIST to assist in avoiding this confusion by expressly stating that the Framework is not designed to be used as a tool for third-party evaluations.

D. Privacy Considerations

Section 7(c) of the Executive Order specifies that "[t]he Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and individual liberties." APPA-LPPC read this passage to specify that NIST must be mindful of privacy concerns with respect to the direction the Framework provides in enhancing security, but not to make privacy a central goal or focus of the Framework.

APPA-LPPC are concerned that, instead of focusing on means to limit the privacy impacts of the Framework, Appendix B appears to recommend independent privacy protections unrelated to the protection of critical infrastructure. The second Governance feature articulated in the "Identify" function of Appendix B, e.g., directs entities to identify policies and procedures that address privacy or Personal Identifiable Information (PII) and to implement procedures which "provide notice to and enable consent by affected individuals." While APPA-LPPC recognize that these provisions are generally consistent with the Fair Information Practice Principles (FIPPs) – and they find these provisions to be generally laudable – it does not appear that their implementation is appropriately the subject of the Framework.

For this reason, APPA-LPPC ask NIST to state in the introduction to Appendix B that its provisions are designed only to call for the implementation of privacy protections to the extent any steps taken in furtherance of the Framework may compromise customer privacy. Protecting the confidentiality of customer data that utilities possess is an important goal for our members, but we ask NIST to recognize that the Executive Order raises this subject in connection with the Framework only to extent privacy may be compromised by the implementation of cybersecurity measures associated with the Framework.

APPA-LPPC note that on December 5, 2013, Harriet P. Pearson provided NIST with an alternative to Appendix B which is generally consistent with the comments herein. That alternative reinforces the point that privacy considerations are important, but should be addressed to the extent impacted by the core concern of the Framework, which is the protection of critical infrastructure.

E. Definition of Adoption

During the Raleigh, North Carolina workshop, a definition of "adoption" for the Framework was provided by DHS and NIST. Participants at the workshop expressed concerns about the use of the word "adopts" and it's definition. The Trade Associations propose the following clarification to the definition posted by NIST on December, 4, 2013.

> An organization adopts the framework when it ***voluntarily uses the Cybersecurity Framework as component of its processes*** (added material italicized) for identifying, assessing, prioritizing, and/or communicating:
>
> - cybersecurity risks,
> - current approaches and efforts to address those risks, and
> - steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities.

The inclusion of the word "voluntary" is consistent with Section 8 of the EO and the establishment of the voluntary program through DHS. Additionally, modifying "key part of its systematic process" to "component of its processes" recognizes that there are sectors that are governed by mandatory and enforceable cybersecurity standards.

F. Further Detailed Comments

APPA-LPPC herewith submit as Attachment C further detailed suggested changes to the Preliminary Framework in the Excel spreadsheet format suggested by NERC for this purpose.

III. CONCLUSION

APPA-LPPC support the work NIST has undertaken to develop a Cybersecurity Framework consistent the EO, and asks that these comments be reflected in the shape of that Framework.

Respectfully Submitted,

AMERICAN PUBLIC POWER ASSOCIATION

/*S*/

Allen Mosher
Vice President of Policy Analysis
and Reliability Standards
Nathan Mitchell
Director, Electric Reliability Standards and Compliance
Delia Patterson
Assistant General Counsel
1875 Connecticut Ave. NW, Suite 1200
Washington, DC 20009
(202) 467-2944
amosher@publicpower.org
nmitchell@publicpower.org

LARGE PUBLIC POWER COUNCIL

/*S*/

Jonathan D. Schneider
Jonathan P. Trotta
STINSON MORRISON HECKER LLP
1775 Pennsylvania Ave. NW, Suite 800
Washington, DC 20006-4605
(202) 728-3034
jschneider@stinson.com
jtrotta@stinson.com

Counsel for Large Public Power Council